AMENDMENT

Amendments to the Claims: Please replace all prior versions and listings of claims with the following listing of claims.

LISTING OF CLAIMS:

1. **(Cancelled)**

2. **(Currently Amended)** The method according to claim [[1]] 37, wherein the identifying information provided in the attack profile identifies a type of communication associated with the detected attack.

3. **(Currently Amended)** The method according to claim [[1]] 37, wherein the identifying information provided in the attack profile identifies at least one of a source Internet Protocol address, a source port number, a destination Internet Protocol address, or a destination port number associated with the detected attack.

4. **(Previously Presented)** The method according to claim 2, wherein the type of communication associated with the detected attack includes at least one of File Transfer Protocol, Simple Mail Transfer Protocol, Telnet, Domain Name System, Windows Internet Name System, HyperText Transfer Protocol, Traceroute, instant messaging, or chat.

5. **(Previously Presented)** The method according to claim 2, wherein the received packets are monitored using Transmission Control Protocol/Internet Protocol at an application layer to characterize the type of communication associated with the packets originating from the source system.

6. **(Currently Amended)** The method according to claim [[1]] 37, further comprising determining the severity of the detected attack based on at least one of a frequency of the

previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attacks, or a volume of the received packets.

7. **(Currently Amended)** The method according to claim [[1]] 37, wherein ~~blocking the packets from being transmitted to the target system includes instructing~~ at least one of a router, a hub, a server, or a firewall is instructed to disable [[a]] the communication channel connecting the source system to the target system.

8. **(Currently Amended)** The method according to claim [[1]] 37, further comprising notifying the source system that the attack has been detected and that a block was placed on packets received from the source system.

9. **(Currently Amended)** The method according to claim [[1]] 37, wherein blocking the subsequently received packets from being transmitted to the target system expires after at least one of a predetermined amount of time, a predetermined period of inactivity, or an occurrence of a triggering event.

10. **(Currently Amended)** A system for protecting a computer network, the system comprising at least one computer ~~readable medium associated with a target~~ device ~~coupled to the network~~, the computer ~~readable medium~~ device having one or more modules, including:

a detection module configured to:

monitor one or more packets received from a source device to determine whether one or more of the received packets include one or more harmful computer code signatures, and to further monitor the received packets to determine whether one or more of the received packets include identifying information that has a history of being included in packets associated with one or more previous attacks directed at [[the]] a target device coupled to the network; and

detect an attack directed at the target device if one or more of the monitored packets include one or more of the harmful computer code signatures, and to further detect the attack if one or more of the monitored packets include the identifying information that has the history of being included in packets associated with the previous attacks directed at the target device;

a scanning module configured to determine a severity of the detected attack directed at the target device;

a log creating module configured to create an attack profile based on information associated with the detected attack, wherein the attack profile provides identifying information included in the monitored packets that include the harmful computer code signatures, and wherein the attack profile further provides the identifying information that has the history of being included in packets associated with the previous attacks directed at the target device; and

a blocking module configured to:

block one or more of the monitored packets from being transmitted to the target device, wherein the blocked packets include the identifying information provided in the attack profile, and wherein the blocking module is further configured to disable a communication channel connecting the source device to the target device to block the packets from being transmitted to the target device; ~~and~~

block one or more subsequently received packets from being transmitted to the target device if the severity of the detected attack exceeds a predetermined threshold, wherein the subsequently blocked packets include packets originating from the source device and packets directed to the target device;

notify a user if the source device originates internally to a defined perimeter of the target device, wherein the user is notified that the communication channel has been disabled and that the attack originated internally to the defined perimeter of the target device; and

enable the communication channel for at least one system that runs a valid application over the communication channel if the source device originates externally to the defined perimeter of the target device.

11. **(Previously Presented)** The system according to claim 10, wherein the log creating module is further configured to store, in a database, identifying information included in one or more packets associated with suspected or confirmed attacks directed at the target device.

12. **(Previously Presented)** The system according to claim 10, wherein the identifying information provided in the attack profile identifies a type of communication associated with the detected attack.

13. **(Previously Presented)** The system according to claim 10, wherein the scanning module is further configured to determine the severity of the detected attack based on at least one of a frequency of the previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attacks, or a volume of the received packets.

14. **(Currently Amended)** The system according to claim 10, wherein the blocking module is further configured to instruct at least one of a router, a hub, a server, or a firewall to disable [[a]] the communication channel connecting the source device to the target device in order to block the packets from being transmitted to the target device.

15. **(Previously Presented)** The system according to claim 14, wherein blocking the subsequently received packets from being transmitted to the target device expires after at least one of a predetermined amount of time, a predetermined period of inactivity, or an occurrence of a triggering event.

16. **(Currently Amended)** A computer device ~~readable medium containing computer executable instructions~~ for detecting and preventing attacks directed at a target system, the computer ~~executable instructions operable~~ having one or more modules that cause the computer device to:

receive one or more packets originating from a source system, wherein the received packets are directed to the target system;

monitor the received packets to determine whether one or more of the received packets include one or more harmful computer code signatures, and further monitor the received packets to determine whether one or more of the received packets include identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system;

detect an attack directed at the target system if one or more of the monitored packets include one or more of the harmful computer code signatures, and further detect the attack if one or more of the monitored packets include the identifying information that has the history of being included in packets associated with the previous attacks directed at the target system;

create an attack profile based on information associated with the detected attack, wherein the attack profile provides identifying information included in the monitored packets that include the harmful computer code signatures, and wherein the attack profile further provides the identifying information that has the history of being included in packets associated with the previous attacks directed at the target system;

block one or more of the monitored packets from being transmitted to the target system, wherein the blocked packets include the identifying information provided in the attack profile, and further to disable a communication channel connecting the source system to the target system to block the packets from being transmitted to the target system; ~~and~~

block one or more subsequently received packets from being transmitted to the target system if a severity of the detected attack exceeds a predetermined threshold, wherein the subsequently blocked packets include packets originating from the source system and packets directed to the target system;

notify a user if the source system originates internally to a defined perimeter of the target system, wherein the user is notified that the communication channel has been disabled and that the attack originated internally to the defined perimeter of the target system; and enable the communication channel for at least one system that runs a valid application over the communication channel if the source system originates externally to the defined perimeter of the target system.

17. (**Currently Amended**) The computer ~~readable medium~~ device according to claim 16, wherein the received packets are monitored transparently in real time.

18. (**Currently Amended**) The computer ~~readable medium~~ device according to claim 16, wherein the received packets are stored in a storage buffer and monitored upon release from the storage buffer.

19. (**Currently Amended**) The computer ~~readable medium~~ device according to claim 16, wherein the one or more modules ~~instructions are~~ further ~~operable~~ cause the computer device to determine the severity of the detected attack based on at least one of a frequency of the previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attacks, or a volume of the received packets.

20. (**Currently Amended**) The computer ~~readable medium~~ device according to claim 16, wherein the one or more modules ~~instructions operable to block the packets from being transmitted to the target system are~~ further ~~operable~~ cause the computer device to instruct at least one of a router, a hub, a server, or a firewall to disable [[a]] the communication channel connecting the source system to the target system in order to block the packets from being transmitted to the target system.

21. (**Currently Amended**) The computer ~~readable medium~~ device according to claim 16, wherein the one or more modules ~~instructions are~~ further ~~operable~~ cause the computer device to notify the source system that the attack has been detected and that a block was placed on packets received from the source system.

22. **(Currently Amended)** The computer ~~readable medium~~ device according to claim 16, wherein blocking the subsequently received packets from being transmitted to the target system expires after at least one of a predetermined amount of time, a predetermined period of inactivity, or an occurrence of a triggering event.

23. **(Currently Amended)** A computer system configured for detecting and preventing attacks directed at terminal devices, comprising:

at least one terminal device;

at least one server coupled to a computer network and to the at least one terminal device, wherein the at least one server is configured to monitor packets directed to the at least one terminal device, the at least one server having one or more modules, including:

a detection module configured to:

monitor one or more packets received from a source device to determine whether one or more of the received packets include one or more harmful computer code signatures, and to further monitor the received packets to determine whether one or more of the received packets include identifying information that has a history of being included in packets associated with one or more previous attacks directed at the at least one terminal device; and

detect an attack directed at the at least one terminal device if one or more of the monitored packets include one or more of the harmful computer code signatures, and to further detect the attack if one or more of the monitored packets include the identifying information that has the history of being included in packets associated with the previous attacks directed at the at least one terminal device;

a log creating module configured to create an attack profile based on information associated with the detected attack, wherein the attack profile provides identifying information included in one or more of the monitored packets that include the harmful computer code signatures, and wherein the attack profile further provides the identifying information that has the history of being included in packets associated with the previous attacks directed at the at least one terminal device;

a scanning module configured to determine a severity of the detected attack directed at the at least one terminal device; and

a blocking module configured to:

block one or more of the monitored packets from being transmitted to the at least one terminal device, wherein the blocked packets include the identifying information provided in the attack profile, and wherein the blocking module is further configured to disable a communication channel connecting the source device to the at least one terminal device to block the packets from being transmitted to the at least one terminal device; ~~and~~

block one or more subsequently received packets from being transmitted to the at least one terminal device if the severity of the detected attack exceeds a predetermined threshold, wherein the subsequently blocked packets include packets originating from the source device and packets directed to the at least one terminal device;

notify a user if the source device originates internally to a defined perimeter of the at least one terminal device, wherein the user is notified that the communication channel has been disabled and that the attack originated internally to the defined perimeter of the at least one terminal device; and

enable the communication channel for at least one system that runs a valid application over the communication channel if the source device originates externally to the defined perimeter of the at least one terminal device.

24. (**Currently Amended**) The computer system according to claim 25, wherein the log creating module is further configured to store, in the database, identifying information included in one or more packets associated with suspected or confirmed attacks directed at the at least one terminal device.

25. (**Currently Amended**) The computer system according to claim 23, further comprising a database coupled to the at least one server.

26. (**Previously Presented**) The computer system according to claim 23, wherein the identifying information provided in the attack profile identifies a type of communication associated with the detected attack.

27. (**Previously Presented**) The computer system according to claim 23, wherein the scanning module is further configured to determine the severity of the detected attack based on at least one of a frequency of the previous attacks, a type of communication used in the previous attacks, an amount of bandwidth usage associated with the previous attacks, or a volume of the received packets.

28. (**Currently Amended**) The computer system according to claim 23, wherein the blocking module is further configured to instruct at least one of a router, a hub, [[a]] the at least one server, or a firewall to disable [[a]] the communication channel connecting the source device to the at least one terminal device in order to block the packets from being transmitted to the at least one terminal device.

29. (**Currently Amended**) The computer system according to claim 23, wherein blocking the subsequently received packets from being transmitted to the at least one terminal device expires after at least one of a predetermined amount of time, a predetermined period of inactivity, or an occurrence of a triggering event.

30. (**Currently Amended**) The computer system according to claim 23, wherein the at least one server is further configured to issue an alert to inform an administrator of the network of the detected attack directed at the at least one terminal device.

31. **(Previously Presented)** The method according to claim 3, wherein the subsequently blocked packets include information identifying one or more of the source Internet Protocol address, the source port number, the destination Internet Protocol address, or the destination port number.

32. **(Currently Amended)** The method according to claim [[1]] 37, wherein the attack profile further provides identifying information included in one or more packets associated with one or more of suspected or confirmed attacks directed at the target system.

33. **(Previously Presented)** The system according to claim 10, wherein the attack profile further provides identifying information included in one or more packets associated with one or more of suspected or confirmed attacks directed at the target device.

34. **(Currently Amended)** The computer ~~readable medium~~ device according to claim 16, wherein the attack profile further provides identifying information included in one or more packets associated with one or more of suspected or confirmed attacks directed at the target system.

35. **(Currently Amended)** The computer system according to claim 23, wherein the attack profile further provides identifying information included in one or more packets associated with one or more of suspected or confirmed attacks directed at the at least one terminal device.

36. **(Currently Amended)** The method according to claim [[7]] 37, wherein disabling the communication channel causes packets that are suspected or confirmed of attacking the target system to be contained within the target system.

37. **(Currently Amended)** A [[The]] method ~~according to claim 7~~ for detecting and preventing attacks directed at a target system, ~~further~~ comprising:

receiving one or more packets originating from a source system, wherein the received packets are directed to the target system;

monitoring the received packets to determine whether one or more of the received packets include one or more harmful computer code signatures, and further monitoring the received packets to determine whether one or more of the received packets include identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system;

detecting an attack directed at the target system if one or more of the monitored packets include one or more of the harmful computer code signatures, and further detecting the attack if one or more of the monitored packets include the identifying information that has the history of being included in packets associated with the previous attacks directed at the target system;

creating an attack profile based on information associated with the detected attack, wherein the attack profile provides identifying information included in the monitored packets that include the harmful computer code signatures, and wherein the attack profile further provides the identifying information that has the history of being included in packets associated with the previous attacks directed at the target system;

blocking one or more of the monitored packets from being transmitted to the target system, wherein the blocked packets include the identifying information provided in the attack profile, and wherein blocking the packets from being transmitted to the target system includes disabling a communication channel connecting the source system to the target system;

blocking one or more subsequently received packets from being transmitted to the target system if a severity of the detected attack exceeds a predetermined threshold, wherein the subsequently blocked packets include packets originating from ~~determining whether~~ the source system ~~originates internally or externally to a defined perimeter of~~ and packets directed to the target system;

notifying a user if the source system originates internally to [[the]] a defined perimeter of the target system, wherein the user is notified that the communication channel has been disabled and that the attack originated internally to the defined perimeter of the target system; and

enabling the communication channel for at least one system that runs a valid application over the communication channel if the source system originates externally to the defined perimeter of the target system.

38. (**Previously Presented**) The method according to claim 9, further comprising correlating a pattern for the detected attack to the severity of the detected attack to determine the amount of time and the period of inactivity after which blocking the subsequently received packets from being transmitted to the target system expires.

39. (**Currently Amended**) The method according to claim 32, further comprising storing, in a database, the identifying information included in the one or more packets associated with the suspected or confirmed attacks directed at the target system.

40. (**Previously Presented**) The method of according to claim 39, further comprising:

scanning the identifying information stored in the database to determine the severity of the detected attack; and

enabling a user to view and modify the severity of the detected attack.

41. (**Previously Presented**) The method of according to claim 39, further comprising scanning the identifying information stored in the database to enable a reaction to the suspected or confirmed attacks based on one or more isolation policies.

42. (**Currently Amended**) The method according to claim ~~[[1]]~~ 37, wherein the attack profile further provides information identifying a time of day and a frequency that that the monitored packets were received.

43. (**Currently Amended**) The method according to claim [[1]] 37, wherein the subsequently blocked packets further include the identifying information provided in the attack profile.

44. (**Currently Amended**) The method according to claim [[1]] 37, further comprising permanently blocking subsequently received packets originating from the source system from being transmitted to the target system if the severity of the detected attack indicates that the source system is a habitual attacker of the target system.

45. (**Previously Presented**) The method according to claim 44, wherein a user can manually reset the permanent block on the subsequently received packets originating from the source system to allow a flow of packets originating from the source system to the target system.